DOI: 10.3969/j.issn.1007-5461.2023.05.011

一种用于量子密钥分发系统的脉冲光致盲攻击防御方案

张 波[1], 瞿迪庆[1], 罗 俊[2], 杜响剑[2], 方余强[3],
蒋连军[3], 高 松[3], 于 林[3], 孙 帆[3], 唐世彪[3*]

(1 国网浙江省电力有限公司金华供电公司, 浙江 金华 321000;
2 国网浙江省电力有限公司东阳供电公司, 浙江 东阳 322100;
3 科大国盾量子技术股份有限公司, 安徽 合肥 230088)

摘 要: 在量子密钥分发系统中,强光致盲攻击利用单光子探测器在实际工作中可能存在因强光导致的线性探测模式, 实现对单光子探测器输出0或1的控制, 从而实施密钥窃取。针对前人提出的新型脉冲光致盲攻击方案可能存在的漏洞, 提出了一种基于分光检测的脉冲光致盲攻击防御方案。在现行通过检测器件工作电流大小来判断是否有强光攻击存在的防御措施基础上, 该方案在单光子探测器被致盲之前实现强脉冲光的100%检测, 从而关闭脉冲光致盲攻击的检测漏洞, 提升量子密钥分发系统的安全性。

关 键 词: 量子信息; 量子密钥分发; 单光子探测器; 致盲攻击; 脉冲光致盲攻击

中 图 分 类 号: O431.2 **文 献 标 识 码:** A **文章编号:** 1007-5461(2023)05-00719-07

A defense scheme of pulse illumination attack for quantum key distribution systems

ZHANG Bo[1], *QU Diqing*[1], *LUO Jun*[2], *DU Xiangjian*[2], *FANG Yuqiang*[3],
JIANG Lianjun[3], *GAO Song*[3], *YU Lin*[3], *SUN Fang*[3], *TANG Shibiao*[3*]

(1 Jinhua Power Supply Company, State Grid Zhejiang Electric Power Co., Ltd., Jinhua 321000, China;
2 Dongyang Power Supply Company, State Grid Zhejiang Electric Power Co., Ltd., Dongyan 322100, China;
3 QuantumCTek Co., Ltd., Hefei 230088, China)

Abstract: In quantum key distribution systems, bright light blinding attack makes use of the detection characteristics of linear mode caused by bright light in the actual work of single-photon detectors to control the output of single-photon detectors to be 0 or 1, so as to implement key stealing. To address the potential vulnerabilities of the new type of pulse illumination attack scheme proposed by previous researchers, a defense scheme against the detector blinding attack by pulse illumination based on beam

基金项目: 安徽省科技重大专项 (202103a13010004)
作者简介: 张 波 (1973 -), 硕士, 高级工程师, 主要从事配电运维、配电自动化方面的研究。E-mail: 402946008@qq.com
收稿日期: 2021-10-25; **修改日期:** 2021-12-23
*通信作者。 E-mail: shibiao.tang@quantum-info.com

split detection is presented. Based on the countermeasures of detecting the working current of the device to judge whether there is a blinding attack, this scheme realizes the detection of bright light pulse with 100% probability before the detector is blinded, therefore, it can close the detection loophole of pulse illumination attack and improve the security of quantum key distribution systems.

Key words: quantum information; quantum key distribution; single-photon detector; blinding attack; pulse illumination attack

0 引 言

基于量子力学基本原理的量子密钥分发 (QKD) 提供了一种原理上无条件安全的通信方式, 通过单光子态随机编码、信道传输和单光子探测等过程, 通信双方通过协商产生完全一致的共享密钥[1]。但是由于现实器件的不完美特性容易被量子黑客攻击利用, 系统的安全性受到挑战[2]。为了提高实用化 QKD 系统的安全性, 关闭系统中现存的漏洞变得尤为关键。近年来, 关于 QKD 系统的攻防策略研究已经逐渐形成体系[3]。在量子黑客攻击手段中, 针对单光子探测器的攻击方案数目最多。

单光子探测器是终端探测的核心设备, 其性能参数直接决定了 QKD 系统的性能指标。理想的单光子探测器拥有 100% 的探测效率, 没有噪声且没有死时间 (无限的带宽)。但实际上单光子探测器受限于所用光电转换器件和后端读出电路, 拥有有限的探测效率 (约 20%) 和暗计数、后脉冲等噪声, 并且带宽有限, 一次响应后需要等待一段时间才能恢复并继续进行下一次单光子探测。针对单光子探测器的量子黑客攻击包括强光致盲攻击[4]、门后攻击[5]、死时间攻击[6]、双计数攻击[7]、超线性攻击[8]等。对于强光致盲攻击, 攻击者通过注入致盲强光使得探测器由单光子探测的盖革模式改变为非单光子探测的线性模式, 线性模式所处的时间区间称为致盲区间。利用线性模式, 攻击者可以再使用脉冲触发光, 使其攻击所采用的不同于接收端测量基矢的探测部分不被发现, 从而消除攻击影响。

本文设计了一种针对强脉冲光致盲攻击探测器的检测方法, 填补了现行检测强光致盲攻击的防御措施漏洞, 可以实现致盲强脉冲光的百分百探测, 从而有效提升 QKD 系统的安全性。

1 现行强光致盲攻击检测方案

为了把单光子探测的盖革模式变为非单光子探测的线性模式, 攻击者向探测器注入用于致盲的强光, 使单光子雪崩二极管 (APD) 输出较大电流, 通过在与 APD 串联的电阻上形成较大压降, 减小 APD 两端电压, 使其低于击穿电压, 从而使 APD 退出盖革模式、进入线性模式。作为接收端, 一般不能阻止外部光注入, 也不能阻止探测器被致盲, 因此防御的原理是确保在探测器被致盲前就能够有效地检测到强光注入。只有光电流足够大时才能导致探测器两端电压下降退出盖革模式, 因此现行的防御措施是检测 APD 的工作电流大小以判断是否有强光攻击。现有的技术方案是在硬件上对给 APD 提供偏压的升压芯片输出电流进行监控。具体地, APD 工作电流超过正常阈值时, 探测器进行告警, 系统停止工作并筛除相关数据。如图 1 所示, 采样电阻对流过 APD 的电流进行采样, 输出电压信号, 并通过 ADC 对该电压信号进行采集, 换算成 APD 的电流大小, 从而监控流过 APD 电流的大小。

上述方案可以有效检测连续光致盲攻击, 但针对新型的脉冲光致盲攻击, 该方案存在漏洞。文献 [9] 提

出了一种针对门控频率40 MHz单光子探测器的强脉冲光致盲攻击方案, 可以有效致盲探测器而不明显增加APD工作电流, 为此需要引入新型防御措施。

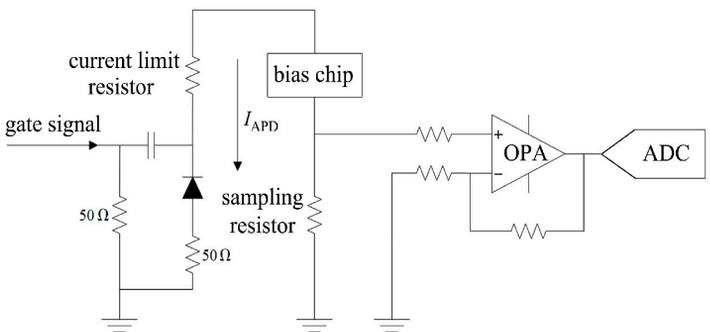

图 1　现行APD工作电流检测方案

Fig. 1　Scheme of current APD working current detection

2　脉冲光致盲攻击检测方案

由于脉冲光致盲探测器时会引入较大的瞬间电流, 该电流在雪崩信号的采样电阻上会产生一个较大幅度的电信号, 可以将采样的雪崩信号功分为两路, 一路用于正常的单光子信号探测, 另一路提高雪崩信号甄别阈值, 正常的单光子信号无法触发甄别, 当APD接收到强脉冲光时, 触发输出脉冲, 可有效监测探测器是否接收强脉冲光, 具体配置如图 2所示。

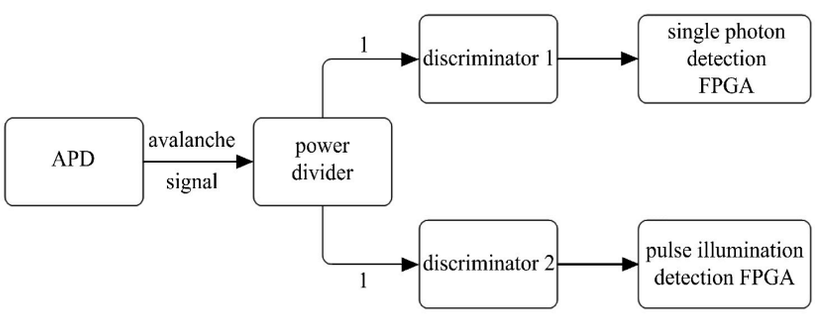

图 2　基于雪崩信号分束的强脉冲光检测方案

Fig. 2　Scheme of pulse illumination detection based on avalanche signal power dividing

上述方案适用于运行在自由运行模式或高速门控模式 (正弦门控和自差分)下的单光子探测器, 在这些单光子探测器中, 进入甄别器的雪崩信号已经滤除门控信号的微分信号噪声干扰, 例如正弦门控模式中门的微分信号通过低通或带阻滤波器进行滤除, 自差分模式中门的微分信号通过功分两路并相对延时一个门周期后做减法进行滤除, 都可以在进甄别器之前得到信噪比良好的雪崩信号, 强脉冲光引发的电流信号也同时被提取出来。

然而对于低速门控模式下的单光子探测器 (如文献 [9] 中提到的门控频率40 MHz的单光子探测器), 一般采用较窄的方波门信号, 经过APD后产生容性响应微分信号, 为一正向和一负向的门噪声信号, 对应门的前沿和后沿, 门的幅度越大、沿摆率越高, 门噪声信号的幅度越大。如图 3所示, 雪崩信号只产生在门内, 幅度与过压相关, 但一般低于门噪声信号幅度, 通常使用符合的方式消除该门噪声信号的影响。然而当攻击者将窄脉冲光的相位设置在门的前沿位置时, 则无法有效区分门微分信号与强脉冲光引发的电流信号。

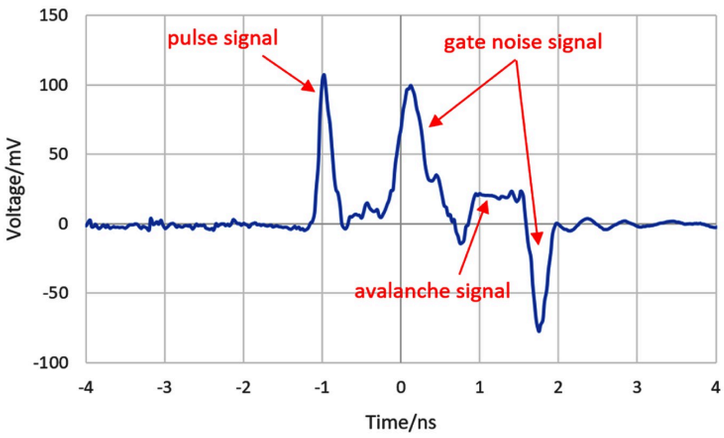

图 3 低速门控的噪声信号与雪崩信号

Fig. 3 Noise signal and avalanche signal in low speed gated mode

为了适应各种电路结构的探测器, 消除强脉冲光致盲攻击的检测漏洞, 提出了一种普适的分光检测方法, 结构如图 4 所示。信号光输入经过一个 9:1 的分束器, “ 9 ” 路仍用于信号光探测, 而 “1” 路用于强脉冲光检测。对于信号光, 该分束器引入约 0.6 dB 的衰减。

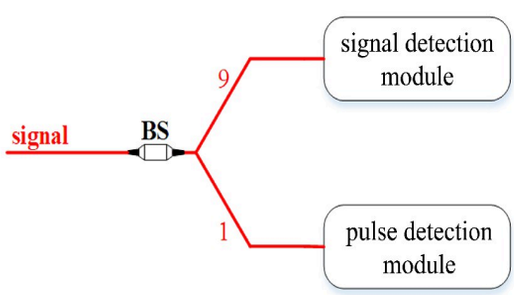

图 4 强脉冲光分光检测方案

Fig. 4 Scheme of pulse illumination detection based on beam splitter

在原探测器系统中增加一个通道, 专用于强脉冲光的检测, 其电路原理图如图 5 所示。相比于高灵敏度的 pin 管, APD 的增益高几个量级, 可以检测到更低能量的脉冲光, 故选用 APD 作为检测电路核心器件。将施加在 APD 两端的偏压 V_b 调节至略低于雪崩击穿电压, 此时 APD 工作在高增益的线性模式下, 这样的设置一方面避免了暗计数对检测的干扰, 另一方面避免了检测路探测器被致盲而无法有效检测的风险。强脉冲光在 APD 上引发的光电流在 1 kΩ 采样电阻上形成的脉冲信号通过交流耦合的方式输入到高速甄别器进行甄别, 再通过高速 D 触发器进行脉冲展宽输入到 FPGA 进行检测。由于线性模式下的 APD 不存在盖革模式下的暗计数, 仅存在暗电流噪声, 高速甄别器的甄别阈值可以设置到略高于电子学噪声, 即可实现针对强脉冲光有无的检测, 当 FPGA 接收到检测通道的探测信号时即说明存在强脉冲光。

搭建如图 6 所示的测试平台对上述方案进行验证。同步的信号源 1 和 2 分别用于触发信号光激光器和攻击脉冲光激光器 [脉冲激光器型号为 QCL-102, 使用武汉光迅的 DFB 激光器, 型号 LD-BF14-1550.12-9-PM-025-1, 波长为 (1550.12±0.10) nm, 输出功率 > 7 mW], 两路光信号通过光纤合束器合束后输入探测器系统 (与文献 [9] 相同的门控频率 40 MHz 的单光子探测器系统, 探测效率约为 20% @1550.12 nm, 暗计数约为 50 cps)。通过两个衰减器调节信号光和攻击脉冲光的光强, 通过功率计标定信号光和攻击脉冲光的功率, 使用 PD 标定信号光与攻击脉冲光的相位。按照如下步骤进行测试: (1) 延时扫描将信号光相位对准门中心位置

(门宽为 1.6 ns), 同时调整攻击脉冲光后沿相位至信号光前 1.25 ns; (2) 打开信号光, 关闭攻击脉冲光, 调整信号光平均每脉冲光子数至 0.3, 记录两个单光子探测器的计数率, 此时信号光探测器为正常计数率, 而攻击脉冲光探测器计数率应为 0; (3) 打开攻击脉冲光, 记录此时两个探测器的计数率, 此时攻击脉冲光功率不足以触发检测探测器, 计数率应仍为 0; (4) 逐渐增加攻击脉冲光功率, 直至检测探测器计数率稳定至攻击脉冲频率值, 记录此时两个探测器的计数率和攻击脉冲光功率, 该功率为能百分百检测攻击脉冲光的最小功率值, 计算得到平均每脉冲光子数; (5) 关闭信号光, 记录此时两个探测器的计数率。

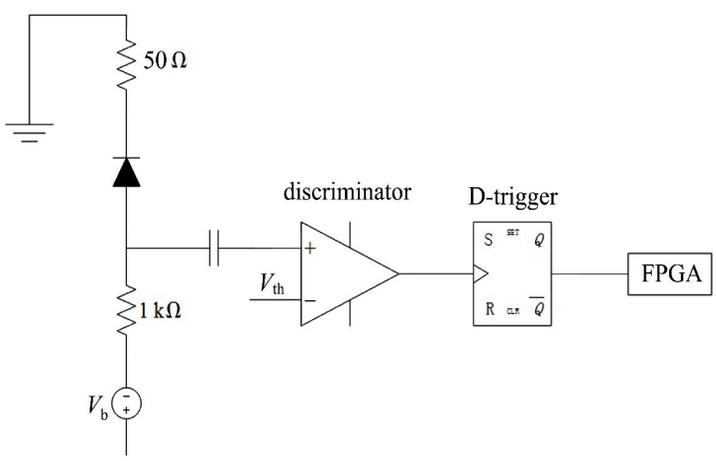

图 5　强脉冲光检测电路原理图

Fig. 5　Scheme of pulse illumination detection circuit

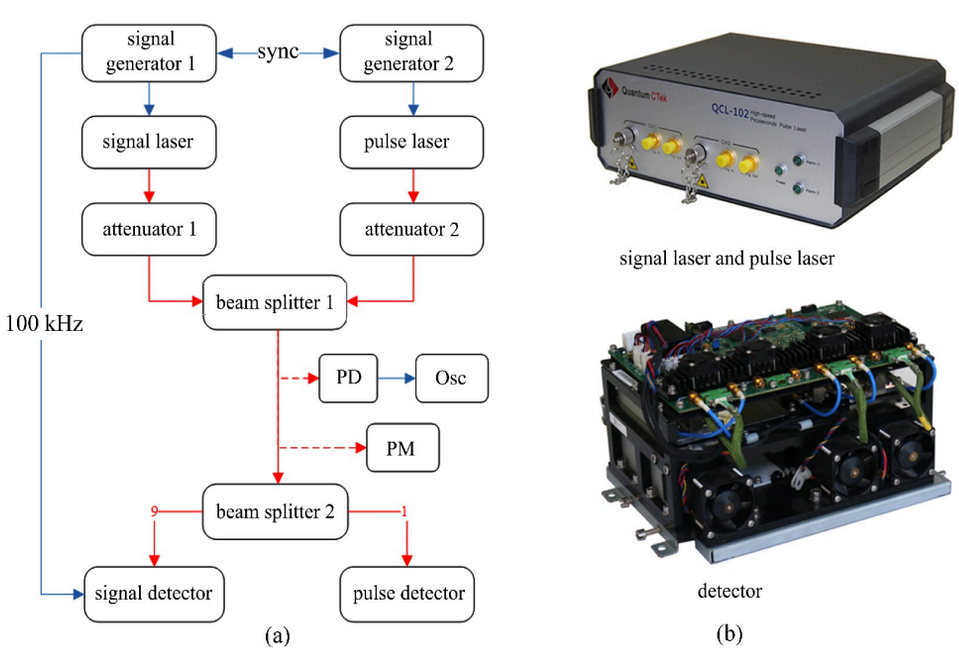

图 6　(a) 强脉冲光检测方案测试平台及 (b) 实验装置实物图

Fig. 6　(a) Scheme of test platform for pulse illumination detection and (b) photos of experimental devices

调整攻击脉冲光激光器输出不同频率的窄脉冲 (脉宽约 250 ps), 按照上述步骤测试得到如表 1 所示的数据。同时模拟文献 [9] 中的攻击方案: 周期间隔为 2 ms, 每 2 ms 内连续 500 个脉冲, 调整每脉冲宽度约 12.5 ns 或 250 ps, 按照上述步骤分别测试得到如表 2 和表 3 所示的数据。

表 1 不同脉冲频率下脉宽约250 ps时的测试数据

Table 1 Test data with about 250 ps pulse width at different pulse frequencies

Pulse frequency /Hz	Step (2)		Step (3)		Step (4)				Step (5)	
	Signal detector count/cps	Pulse detector count/cps	Signal detector count/cps	Pulse detector count/cps	Signal detector count/cps	Pulse detector count/cps	Energy of pulses/dBm	Photon number of per pulse	Signal detector count/cps	Pulse detector count/cps
1000	261275	0	259683	0	263745	1000	−81.57	5.43×10^4	51	1000
10000	261112	0	261090	0	263430	10000	−71.51	5.51×10^4	154	10000
100000	259314	0	261330	0	264142	100000	−60.54	6.89×10^4	1310	100000
1000000	260691	0	260366	0	269911	1000000	−50.8	6.49×10^4	6264	1000000

表 2 脉冲光脉宽约12.5 ns时模拟文献 [9] 攻击方案的测试数据

Table 2 Test data of attack scheme in literature [9] are simulated when pulse width is about 12.5 ns

Pulse width/ns	Step (2)		Step (3)		Step (4)				Step (5)	
	Signal detector count/cps	Pulse detector count/cps	Signal detector count/cps	Pulse detector count/cps	Signal detector count/cps	Pulse detector count/cps	Energy of pulses/dBm	Photon number of per pulse	Signal detector count/cps	Pulse detector count/cps
12.5	262911	0	267770	0	270008	250000	−44.1	1.21×10^6	7002	250000

表 3 脉冲光脉宽约250 ps时模拟文献 [9] 攻击方案的测试数据

Table 3 Test data of attack scheme in literature [9] are simulated when pulse width is about 250 ps

Pulse width/ps	Step (2)		Step (3)		Step (4)				Step (5)	
	Signal detector count/cps	Pulse detector count/cps	Signal detector count/cps	Pulse detector count/cps	Signal detector count/cps	Pulse detector count/cps	Energy of pulses/dBm	Photon number of per pulse	Signal detector count/cps	Pulse detector count/cps
250	260876	0	262161	0	265647	250000	−59.62	3.40×10^4	1626	250000

由表 1 数据可以得出: 对于不同频率的攻击脉冲光, 检测探测器的计数率与脉冲光频率相同 [步骤 (4) 的第 2 列数据), 说明攻击脉冲光在每 ns 约 10^5 量级光子数下可被全部探测。同时, 信号光探测器计数率随着脉冲光频率增加而增加。从步骤 (5) 关闭信号光的数据可以看出, 信号光探测器计数率的提升源于攻击脉冲光的影响。根据文献 [10] 的分析, 光信号在探测器门控信号外线性模式下触发的载流子会延迟到门内释放从而引发雪崩, 带来额外计数。

从表 2 和表 3 的数据中可以得出:模拟文献 [9] 中的攻击方案, 攻击脉冲光可被完全检测, 且检测的脉冲光强度远小于信号光探测器被致盲所需 10^7/ns 量级光子数。同时, 相比于文献中的 4 ns 攻击脉冲光脉宽, 更宽或更窄的脉冲光都能被有效检测。

3 结 论

所提出针对 QKD 系统探测器的强脉冲光致盲攻击检测方法可以检测到约 10^5/ns 量级光子数的脉冲光, 而实现致盲单光子探测器需要更多的光子数, 以使强脉冲光致盲攻击的检测漏洞被完全关闭。该检测方法可以应用到所有类型探测器的 QKD 系统中, 有效提升了 QKD 系统的安全性。

参考文献:

[1] Bennett C H, Brassard G. Quantum cryptography: Public key distribution and coin tossing [C]. *Proceedings of the International Conference on Computers, Systems and Signal Processing*, Bangalore, India, 1984: 175-179.

[2] Brassard G, Lütkenhaus N, Mor T, *et al*. Limitations on practical quantum cryptography [J]. *Physical Review Letters*, 2000, 85 (6): 1330-1333.

[3] Xu F H, Ma X F, Zhang Q, *et al*. Secure quantum key distribution with realistic devices [J]. *Reviews of Modern Physics*, 2020, 92(2): 025002.

[4] Lydersen L, Wiechers C, Wittmann C, *et al*. Hacking commercial quantum cryptography systems by tailored bright illumination [J]. *Nature Photonics*, 2010, 4(10): 686-689.

[5] Wiechers C, Lydersen L, Wittmann C, *et al*. After-gate attack on a quantum cryptosystem [J]. *New Journal of Physics*, 2011, 13 (1): 013043.

[6] Weier H N, Krauss H, Rau M, *et al*. Quantum eavesdropping without interception: An attack exploiting the dead time of single-photon detectors [J]. *New Journal of Physics*, 2011, 13(7): 073024.

[7] Lütkenhaus N. Security against individual attacks for realistic quantum key distribution [J]. *Physical Review A*, 2000, 61(5): 052304.

[8] Lydersen L, Jain N, Wittmann C, *et al*. Superlinear threshold detectors in quantum cryptography [J]. *Physical Review A*, 2011, 84(3): 032320.

[9] Wu Z H, Huang A Q, Chen H, *et al*. Hacking single-photon avalanche detectors in quantum key distribution via pulse illumination [J]. *Optics Express*, 2020, 28(17): 25574-25590.

[10] Calandri N, Sanzaro M, Tosi A, *et al*. Charge persistence in InGaAs/InP single-photon avalanche diodes [J]. *IEEE Journal of Quantum Electronics*, 2016, 52(3): 1-7.